REPORT ON RECOMMENDATIONS OF THE DIGITAL TRANSFORMATION WORKING GROUP OF THE IX SUMMIT OF THE AMERICAS[1]

---

1. The recommendations contained in this document were formulated by the members of the thematic working groups of the following subregions: i) Canada, the Caribbean, and the United States, ii) Mesoamerica and iii) South America

Working Group Digital Transformation of Canada, the Caribbean and United States

I.   Introduction

Members of **The Digital Transformation Working Group (Canada, USA, and the Caribbean)**, including Equality Now, Equality Bahamas, Latino Community Foundation, RespectAbility, Organization for Social Media Safety, and Rotary International respectfully submit this report in advance of The IX Summit of the Americas. The effective recommendations provided in this report should be adopted to strengthen and complement The Draft Political Commitment for the Ninth Summit of the Americas: Regional Agenda for Digital Transformation.

II.   Recommendations

Commitment 1: To facilitate affordable, universal broadband access to the Internet for all peoples of the Americas by 2030

Governments must prioritize reliable, accessible, affordable, and meaningful connectivity, regardless of ability to pay, for their citizens in order to secure the benefits of an inclusive digital society for everyone. In order to form a thriving digital ecosystem, governments must adopt a comprehensive human rights-based approach that aims at closing the digital divide.

Internet usage is growing with the expansion of 5G technology in many regions including within the Americas. Unfortunately, meaningful connectivity is still a challenge. In 2021, the International Communication Union (ITU), reported that nearly 3 billion people have never used the Internet. The majority of those offline are women, thereby reinforcing gender inequalities.

Men remain 21% more likely to be online than women, rising to 52% in the world's least developed countries (LDCs). Governments have not adequately developed policies to address the digital gender gap.

Until we manage to close this significant gap, we cannot meet the Sustainable Development Goal target 9.c for universal Internet access. To be offline means missing out on learning and earning, accessing valuable services, and participating in democratic public debate. The digital divide deepens existing gender inequalities, pushing women further to the margins of society.

Recommendations

We encourage Governments to:

- Acknowledge, particularly in the context of the COVID-19 pandemic, that access to broadband Internet is a human right.[2]
- Adopt measures to ensure everyone has equal access to a secure and open Internet by addressing factors such as level of employment, education, poverty, literacy, migrant status, race, and geographical location that disenfranchise women and other groups.

---

2 See, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La of 16 May 2011, A/ HRC/ 17/ 27)

- Adopt policies and regulations that foster universal and equitable access to the Internet, including fair and transparent market regulation, universal service requirements and licensing agreements.
- Strengthen universal access strategies with modern, ambitious Universal Service & Access Fund3 mandates, and include institutional coordination in the policy design and implementation stages.
- Universal broadband access is accompanied with universal connection to the Internet. 'Access' can be misused by ISPs seeking to present unconnected Wi-Fi, fiber, and infrastructure as access in order to gain market image and gain favor from governments interested in universal connectivity. Connectivity must not rely on redundant systems such as in-ground fiber and Wi-Fi hotspots/units installed on streetlights, buildings, and street furniture.
- Provide free public Internet in low-income areas and city centers to increase access for people experiencing poverty
- Ensure high quality, consistent Internet access in rural areas.
- Provide flexible subcontracting opportunities for community-led nonprofits, recognize, and tackle linguistic barriers, and involve ethnic media partnerships to advertise broadband funding programs.
- Develop a universal standard of acceptable Internet speeds to ensure high quality and consistent Internet use for all, while recognizing that the current standards are too low.

Commitment 2: **To expand digital government transformation and improve the digital literacy and cybersecurity capacity of citizens, civil society, the private sector, and other stakeholders**

Recommendations

We encourage Governments to:

- Acknowledge that digital literacy and cybersecurity needs reflect the social dynamics found online-including how both anonymity and 'influencer' status create space for new and old forms of predatory practices (e.g., predatory financial services, misinformation, harassment, isolation)-and address them. By proactively monitoring trends online, key trusted figures can disseminate reliable actions to the public and leverage well-known, neutral stakeholders.
- Provide training and programs for digital literacy and cybersecurity to the public and incentivize members of the private sector and civil society organization to do the same, prioritizing people in situations of vulnerability including women, youth, elderly people, LGBTQ+ people and human rights defenders.
- Combine digital literacy with provision of devices, Internet access, and other necessary resources and services, such as bank accounts, to enable participation.
- Develop both programs and alternatives for older people who have not engaged with smart devices or used the Internet and implement a policy to prevent them from being forced to transition to digital platforms for the benefit of service providers.

---

3 See, Universal Service & Access Funds: An Untapped Resource to Close the Gender Digital Divide, March 2018, <available at:
https://webfoundation.org/docs/2018/03/Using-USAFs-to-Close-the-Gender-Digital-Divide-in-Africa.pdf&gt

Commitment 4: To expand opportunities for businesses, particularly small and medium-sized enterprises, to participate in e-commerce and utilize digital technologies and logistics services to improve their operations
Recommendations

We encourage Governments to:

- Prioritize micro-businesses such as small shops, street vendors, and individuals operating hyper-local businesses which have a greater need for low-cost Internet connection and use the opportunities available online.
- Provide and encourage the development of grants and initiatives to increase access to digital technology and enable and increase participation in digital economies.

Commitment 7: To promote respect for human rights on the Internet and in the dissemination and use of emerging and digital technologies

a. Towards a Universal Declaration on Digital Rights

The rapid expansion of digital technology is bringing extraordinary opportunities as well as profound disruption to our global society. The need to recognize access to broadband Internet as a human right is greater than ever.

As we accelerate into our digital future-of fast paced digital transformation, high Internet speeds, algorithms, machine learning, web 3, the blockchain and the metaverse-this new ecosystem is reflecting, replicating and indeed amplifying the biases and discrimination of existing structural inequalities of the physical world, such as racism and misogyny. Online channels have created tremendous opportunities for free expression, organizing and collective action on a global scale and for countering oppression; however, rights and freedoms are infringed upon, existing discriminations and biases are amplified, and old and new forms of violence and crime are perpetrated online in globalized multijurisdictional, barely regulated space with increasing impunity. International and national laws and systems fail to keep pace with technological advances and their consequences.

A bold, transformative, universally agreed and feminist Declaration on Digital Rights grounded in international human rights law and principles will help ensure that the rights of all people, particularly the most vulnerable and those who suffer systemic discrimination, are protected in the digital space.

Recommendations

We encourage Governments to:

- Develop[4] an intersectional feminist Universal Declaration on Digital Rights-implemented through robust national laws-that articulates the rights of all people in the digital space, guarantees protection of fundamental rights, regulates human

---

4. In collaboration with other governments, the United Nations, the OAS, INTERPOL and industry, and other stakeholders particularly the technology industry and civil society organizations.

interactions, and addresses the accountability of governments, the technology industry and other players responsible for this space. It must specifically address the needs of marginalized people including people with disabilities, ensuring that the technologies in use are accessible.

- Provide safeguards that protect online users from threats of violent social media interactions such as, cyber bullying, disinformation, privacy violations.
- Commit to preventing and eliminating online harassment and violence, recognizing this disproportionately affects women, LGBTQI+ people, and young people.

b. Addressing online violence against women and girls

Today, the scope and scale of Internet and digital connectivity and increasingly affordable access to camera ready technology, coupled with gendered notions of male entitlement and the intensification of misogyny online, is enabling online violence against women, girls and children to occur at unprecedented levels across the world.

Key challenges to addressing online sexual exploitation and abuse (OSEA) include:

- Many laws pre-date important technological advances, such as camera-ready technology, and do not adequately respond to the Internet's global and ever-evolving nature.
- Inconsistencies internationally and nationally in definitions of OSEA, and the application of digital service providers' and platforms' terms and conditions for use, make it difficult to identify and prosecute perpetrators.
- Measures to prevent and detect OSEA have been mostly left to digital service providers and platforms because of the different contractual, criminal, and private law obligations placed on them in different countries. Consequently, there has been heavy reliance on voluntary measures implemented by digital service providers and platforms.
- There is an inherent tension between digital rights and freedoms, such as privacy and freedom of expression, and the right to protection and safety from online harm.
- Investigating and prosecuting cases of sexual abuse and exploitation is extremely challenging for law enforcement, partly because criminal activity is often not confined to one country or territory. Complex cases can involve multiple offenders and/or victims, various platforms, in different countries.

Recommendations

We encourage Governments to:

- Review and update national and regional legislation and policies to ensure that they are aligned to the digital age and fully protect people from online violence including gender-based violence such as image-based sexual abuse, doxing, and technology-enabled sex trafficking.
- Adopt legally binding standards that clarify the role, responsibility, and accountability of digital service providers and platforms, in preventing, detecting, and reporting online violence and sexual abuse on their platforms.
- Strengthen national capacity and international cooperation to prevent, detect and prosecute cases of online violence.

- Conduct up-to-date research and analysis on online violence against women and girls, including online sexual exploitation and abuse.
- Protection and access to justice for human rights defenders.

Commitment 9: To promote transparency and accountability in the use of digital technology, including the responsible and ethical use of trustworthy artificial intelligence, while protecting privacy and human rights

Today, privacy is not just about one's data. Developers can aggregate data about a person to train a machine learning model that is subsequently used to make predictions about other people. Organizations may use these correlative patterns to classify data into groups. It then becomes possible to probabilistically infer those other individual cases are like or unlike members of the group, such that a particular categorization does or does not apply to a third party who was not in the original data set. This result disempowers individuals about whom inferences are made and who have no control over the data sources from which the inferential model is generated. Machine learning thus exposes the need to recognize two categories of data: one, personal data, and two, data that can be processed to make inferences about persons.

Threats include, but are not limited to:

- Invasions of privacy and data breaches, which include the non-consensual sharing of intimate images, searching for and publishing private or identifying information about a particular individual on the Internet, or the mass disclosure of private information through hacking.
- Biases which include sex and race discriminatory recruitment practices, gender and racial biases (that alarmingly range from insurance offers to predicting someone's propensity for criminal behavior), and lack of diversity in the data used to train machine learning systems, which can produce discriminatory outputs from artificial intelligence (AI) systems making decisions about people's lives and the information people are fed.
- Machine learning provides pathways to use data and make probabilistic predictions-inferences-that are inadequately addressed by the current regime. At this present time, it is possible to aggregate myriad individuals' data within machine learning models, identify patterns, and then apply the patterns to make inferences about other people who may or may not be part of the original data set.

Also, the use of algorithmic decision-making systems is often not apparent to the end user at first sight. Additionally, information regarding the systems, including the processes, relevant documentation, and accountable persons, is not readily accessible to independent individuals and entities in order for them to be able to be informed and seek recourse and redress.

Recommendations

We encourage Governments to:

- Adopt legally binding regulations and standards governing the use of AI in the public and private sector, including providing redress to citizens negatively impacted by AI systems.

- Mandate Human Rights Impact assessments for technologies used in public administration and potentially carrying risks of harm to citizens.
- Administer and set guard rails for AI programmers to mitigate the risk of face-recognition discrimination and coding biases.
- Develop frameworks to ensure collaboration between the technology sector and other sectors including law enforcement, civil society organizations and academia on principles and practices that will promote responsible and ethical use of artificial intelligence.

Commitment 11: To prevent the shutting down, blocking, or throttling of Internet, telecommunication, or social media platforms;

Mostly driven by political and national security concerns, Internet shutdowns are a growing pandemic. The Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue regarded Internet shutdowns, regardless of the justification, a violation of Article 19(3) of the International Covenant on Civil and Political Rights because the interruption to Internet access is disproportionate. The Report called on States to ensure maintenance of Internet access at all times, including during times of political unrest.

It has also been found by the Internet Society (ISOC) that Internet shutdowns not only have a human rights impact but a technical and economic one as well. By shutting down the Internet users' trust is undermined which sets in motion a number of consequences for the local economies, including impacting the reliability of critical e-government services, accessing key public health information and restricting online participation for even the most mundane of tasks. Internet shutdowns affect many sectors of society.

Recommendations

We encourage Governments to:

- Condemn Internet shutdowns, particularly through country-specific statements issued during regional and international human rights platforms and sessions.
- Adopt measures to ensure that Internet shutdowns are not permitted on any grounds, including public order or national security grounds. The measures should require Internet intermediaries to be transparent about any traffic or information management practices they employ.
- Build resilient infrastructure by distributing more Internet exchange points, along with increased diversity of Internet connectivity at international borders to frustrate efforts of Internet shutdowns.
- Highlight the impact of Internet shutdowns on civil and political rights and increase awareness and attention of such human rights violations on economic, social and cultural rights, particularly linking to the broader achievement of the UN Sustainable Development Goals and the 2030 Agenda through the Broadband Commission and High-level Political Forum on Sustainable Development (HLPF) studies.

Commitment 12: **To collaborate on the development and implementation of interoperable, standards-based policies for cybersecurity and consumer protection, including safeguards to prevent and address cybercrime;**

Due to the complex nature of cyber breaches and crimes-occurring across borders and not only impact national security, companies' integrities but the protection of consumers' rights and interests-there is a need for measures and tools that include policies, security safeguards, guidelines, technologies, and best practices that are used to protect the cyber environment, computer and ICT systems, organizations, and users' assets.

In the development and implementation of these policies, there must be a proper balance between the interests of law enforcement and respect for fundamental human rights, such as the right to freedom of expression, privacy and protection of individuals, as enshrined in applicable international and regional human rights treaties.

Recommendations

We encourage Governments to:

● Increase capabilities, particularly in law enforcement by expanding understanding of police and judicial officers about cybercrimes and equipping them with tools to investigate and prosecute criminals.
● Strengthen regional and international cooperation and dialogue between States, the United Nations, the OAS, INTERPOL, the technology industry, civil society organizations and other stakeholders.
● Review and update national legislation and policies to ensure that there are no gaps in law that result in infringement of fundamental human rights in the name of protection from cybercrime or cybersecurity.
● Prevent cybercrime (financial, mental, physical, etc.) and crimes with a digital component by creating standards that include third party experts for research analysis, data collection from affected sub-populations (e.g., young students, seniors, low-income families), and oversight of app security measures which can protect populations.

III. Contributors

This report was made by civil society members of **The Digital Transformation Working Group (Canada, USA, and the Caribbean)**. Please find information about some of the contributing organizations below:

Equality Now is an international human rights NGO and a registered civil society organization of the Organization of American States (OAS). Equality Now's mission is to achieve legal and systemic change that addresses violence and discrimination against all women and girls around the world. Founded in 1992, Equality Now is a global organization with partners and supporters in every region. Ending sexual violence, ending sexual exploitation, ending harmful practices and achieving legal equality are the main areas **of** Equality Now's work. Regarding digital transformation, Equality Now works to ensure that the human rights of all women and girls are fully realized in the digital world and that governments and the private sectors proactively work to combat online sexual exploitation and abuse of women and girls.

Equality Bahamas is a feminist organization promoting women's and LGBTQI+ people's rights as human rights through advocacy, public education, and community engagement. It uses international and regional mechanisms such as Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) and Belém do Pará to advocate for constitutional and legislative reform, feminist policymaking, and development of **programs** and services in recognition and toward the expansion of human rights. Its work prioritizes people in situations of vulnerability including young people, people experiencing poverty, informal workers, people with disabilities, and migrant people. Digital transformation is in progress and there must be a feminist approach to ensure that these communities are not left behind or their vulnerabilities exacerbated. They must be centered, and it must be recognized that until they have full access-including properly functioning devices, reliable Internet connection, digital literacy, and tools and services such as banking and payments systems-digital transformation is not complete, equitable, or effective and these systems cannot be used to the effect of their exclusion or inability to participate.

Latino Community Foundation is a philanthropic nonprofit organization whose sole mission is to build an ecosystem of civically engaged philanthropic leaders, investing in Latino-led organizations, and increasing civic and political participation by **Latinos** in California. To date, LCF has invested nearly $20 million to build Latino leadership in the state. Between 2010-2016, the LCF campaigned to increase broadband adoption rates in underserved, low-income Latino communities in the state. LCF launched the ***Get Latinos Connected Campaign***, a campaign that successfully connected 2,135 Latinos to the Internet, provided training to more than 5,000 Latino families, and ensured greater access to hardware for low-income families. The campaign focused on creating a culture of technology and educated Latino families about available low-cost hardware and Internet options. LCF also trained and deployed a cohort of 26 community tech promotors (community outreach workers) that worked in key Latino communities to help sign up families to low-cost Internet at home and troubleshoot their tech needs.

Respectability is a diverse, disability-led nonprofit that works to create systemic change in how society views and values people with disabilities, and that advances policies and practices that empower people with disabilities to have a better future. People with disabilities make up the largest minority group in the United States. Disabilities increase the digital divide in affected populations due to insufficient financial resources or skills and tools which would enable them to fully benefit from Internet access. This low accessibility to Internet resources may itself be another factor limiting its use by people with disabilities. We support digital accessibility: the inclusive practice of removing barriers that prevent interaction with, or access to websites, digital tools and technologies, by people with disabilities**.**

Organization for Social Media Safety is the first consumer protection organization exclusively focused on social media. We work to make social media safe for everyone. We protect against all social media-related dangers including depression/suicide, hate speech, sexual crimes, human trafficking, propaganda and anti-democratic practices, and cybercrimes. We work with academic institutions and global partners to identify evidence-based practices, recommendations, and strategies for individuals, families, schools, government agencies, and those impacted by the social dynamics influenced by social media platforms. The digital world is growing more interconnected and touches every part of our lives. Without proactive monitoring and resources to prevent malicious actors online, our families, friends, neighbors, and democratic institutions are at risk. As universal connection to the Internet grows, our efforts to protect through education, advocacy, and technology extends across cultures, languages, and countries.

Mesoamerica Digital Transformation Working Group

Emphasizing the Inter-American Democratic Charter ratified by all member states, we suggest the application of the instruments, treaties, decrees, and resolutions in their countries of origin.

Recalling the Declaration of Quebec City of 2001, which affirms that upholding and the strengthening of the rule of law and strict respect for the democratic system are both a shared purpose and commitment, we request and propose to the governments of the Americas that they modify the text of the Draft Political Commitment for the IX Summit of the Americas Regional Program for Digital Transformation, prior to its approval, in accordance with the proposal put forward by Civil Society Organizations and Actors.

Creating controls on the use of platforms that protect the confidentiality and privacy of individuals' personal data to prevent them from being used for other purposes without their consent (in countries with dictatorships) based on the Universal Declaration of Human Rights.

Draft Political Commitment for the IX Summit of the Americas Regional Program for Digital Transformation

We, the Heads of State and Government of the Americas,

AFFIRMING the essential role of dynamic and resilient digital ecosystems for supporting thriving digital economies by modernizing preparedness and response to address climate change and health phenomena, combating corruption, promoting inclusion of all peoples, fostering and protecting above all respect for everyone's dignity, respect for fundamental human rights and freedoms, electoral and judicial processes with audited digital systems geared to transparency; increasing competitiveness and preventing monopolies, and paving the way for investment and improving public services;

EMPHASIZING that the 2019 Coronavirus pandemic (COVID-19) highlighted the magnitude of the digital divide by underlining the importance of Internet access, digital education, access to public services, access to a virtual health consulting portal, digital jobs with transparency, and security in the use of digital tools, especially among economically vulnerable, marginalized, or rural communities. Promoting the application of international instruments on transparency in the digitization of state data, which should be audited before, during and after that process, in accordance with international treaties and anti-corruption resolutions.

RECOGNIZING the need for greater regional cooperation, including cooperation among the private sector, civil society and other social actors, to formulate policies that shape digital ecosystems to increase economic growth, regional competitiveness, and responsible and ethical use of technology, while observing human rights;

We hereby undertake to:

1.   Facilitate competitively priced, universal broadband Internet access to all peoples of the Americas by 2030;

2.   Expand the transformation of digital governance to include open-signal telecommunications, authorized by each member state and that form part of the private telecommunications company. Respect privacy and human rights, while creating anti-corruption and transparency tools; improving digital education, and the cybersecurity capabilities of citizens, civil society, the private sector, and other stakeholders;

3.   Strengthen cooperation on responsible digital trade that does not violate human rights, including commitments to facilitate cross-border data flows, while ensuring the protection of privacy;

4.   Expand opportunities for companies, without discrimination, especially small and medium-sized enterprises, to participate in e-commerce, use digital technologies and digital logistics services to improve their operations, while maintaining ethical standards, privacy, and respect for the law.

5.   Promote financial inclusion through the use and acceptance of digital payment platforms, at the commercial and state level, as well as broader, optional digital banking services for citizens; especially in rural and indigenous populations that do not have access to traditional financial services subject to regulations on transparency, anti-corruption, and money laundering while maintaining standards of ethics, privacy, and equity for all.

6.   To advance the use of digital tools and platforms to expand equity, inclusion, and access to the Internet for the citizens of the member states thereby reducing the digital divide, including through greater and more inclusive use of e-government, e-commerce, financial, health, educational, civic participation, and cultural preservation technologies, with a focus on strengthening human rights and privacy.

7.   Promote respect for human rights, the dignity of individuals, privacy and the laws of each state, and their application in the use of the Internet and in the dissemination and use of emerging and digital technologies; criminalizing and penalizing digital violence and cybercrime in the legislation of the States to ensure safe virtual environments for all people without discrimination.

8.   Apply digital tools that include the digitization of open signal television media with frequencies authorized by each member state to prepare for and respond efficiently to critical incidents involving, *inter alia*, health, climate, environment, the economy, and violation of human rights.

        a) Encourage the protection and support of television and radio media, with the radio spectrum allowed in each member state, since they communicate to a specific segment of the population that has difficulty in acquiring the Internet, as was evident during the pandemic and the natural risk alerts.

9.   Ensure that the member states guarantee transparency based on the accreditation of legitimate governments to the OAS, accountability in the use of digital technology, including the ethical use of reliable artificial intelligence, while protecting the dignity of individuals, privacy, and human rights; with accountable governments.

a) Demand from the providers of social platforms and networks the mechanisms that guarantee the above-mentioned protection.

b) Strengthen administrative, economic, fiscal, and security mechanisms in the use of personal and commercial information, to prevent the use of artificial intelligence, algorithms, or interoperability to unilaterally influence the manipulation of social behavior, especially in relation to the manipulation of educational content, moral content, public opinion, and electoral preferences.

c) Encourage the use of digital technology in electoral matters where these are independent of the branches of government of the member states, accredited by the OAS and audited before, during, and after an election with transparent results. The necessary measures shall also be adopted to safeguard personal data and other sensitive information generated or compiled through the use of electoral technology, in order to prevent them from being used for other purposes without the consent of the persons concerned.

d) Establish and implement the international resolutions adopted by the OAS on auditing, transparency, and efforts to combat corruption with inclusion of governments in coordination with the Inter-American e-Government network or maintain their commitment to Open Government Partnership (OGP), so as to promote measures to prevent and detect conflicts of interest based on the Inter-American Convention Against Corruption.

10.   Support the development of open, interoperable, secure, and reliable communication network structures. Ensure that member states develop regulatory policies that expand connectivity, promote competition, and foster innovation.

a) Require platform providers to furnish mechanisms that guarantee the protection of personal data.

b) Encourage implementation of the use of open digital television networks approved by the member states

11.   Avoid shutting down, blocking, or throttling Internet, telecommunications, or social networking platforms; unless:

a) they violate the human rights, protection, and safety of children, or contravene the Inter-American Observatory regulations on the Sexual Exploitation of Children and Adolescents for commercial gain.

b) Ensure the blocking of any pornographic material that promotes sexual violence, psychological violence, sexual exploitation, human trafficking, pedophilia, child abuse, increased criminality, and other offenses by applying protocols protecting women, children, adolescents, older adults, people with disabilities, and the LGTBI community. (Based on the American Declaration of the Rights and Duties of Man, the American Convention on Human Rights and other inter-American protection instruments containing principles and rights relating to LGTBI people.)

c) Ensure protection of telecommunications as a human right guaranteeing free expression in each country based on the universal declaration of human rights and political constitutions or magna carta of each country. Technology can be

used to incorporate telecommunications in digital platforms, not to get rid of them.

12.   Collaborate in the development, implementation of interoperable policies based on cyber security, protection, and consumer privacy standards, including the Joint Declaration on Freedom of Expression, and the Internet adopted at the OAS, political constitutions or charters and universal declaration of human rights in order to safeguard, prevent, and address cybercrime and all activities conducive to citizens engaging in unethical or undemocratic practices.

13.   Develop and implement by 2023 in the region the application of digital programs for transformation in the Americas based on the present shared commitments, and

14.   Mandate ministers and competent authorities, with the support of the members of the Joint Summit Working Group and OAS Electoral Affairs Group, to ensure, with a focus on resolutions adopted and on the Inter-American Democratic Charter, that technology is used correctly in the electoral processes to support the process of determining and implementing the program through the Summits of the Americas Process via the Summit Implementation Review Group.

South America Digital Transformation Working Group

Introduction

The purpose of this document is to systematize the positions and contributions of a wide range of social actors and civil society organizations. Stakeholders and organizations conveyed their approaches and opinions regarding digital transformation in the Americas using the participation channels provided.

Main contributions and positions:

Digital transformation implies **digital access** as a human right, with an open, interoperable and secure internet network, and with broad access to digital technologies, ensuring the digital inclusion of all members of society. Multisectoral strategic partnerships are recommended to expedite the building of an Internet infrastructure to improve access and foster the development of the Internet ecosystem.

Digital transformation should seek to promote **transparency and accountability** in the design and use of digital technology. This includes the responsible and ethical use of Artificial Intelligence (AI) and the establishment of independent audits with a human rights approach for the largest technology platforms.

This is indispensable now that in recent years countries with authoritarian governments have passed control laws enforced with the use of technology, such as classification of the population by social scores, with punishments that include restrictions on mobility and limited access to basic resources, and even partial or total seizure of economic assets, accompanied by censorship of all manifestations of freedom of expression. Therefore, it is essential that the Inter-American Commission on Human Rights set specific standards for the Hemisphere to ensure respect for human rights on the Internet, as well as the use and impact of emerging and digital technologies, including the protection and privacy of personal data of citizens, especially groups and civil society organizations involved in whistle blowing, monitoring, and control.

A rights-based approach to digital transformation can lead to the **recognition and protection of rights** such as: digital citizenship, personal information management, virtual privacy, the right to privacy (*derecho al olvido*) and anonymity, cyber peace and information security, privacy in the digital environment, internet neutrality, digital security, freedom of digital expression, education, and digital literacy.

For the success of digital education and health measures, digital transformation must ensure electricity **coverage**, Internet access, devices that allow access to the network and, above all, make it possible to implement training programs to ensure digital **literacy**. Priority needs to be given to implementation in communities with less accessibility and to the most vulnerable groups (remote rural areas, indigenous groups, people with disabilities, older adults, and so on), in order to improve the quality of life and citizens' access to rights (access to health care, education, work, social participation, etc.).

Regarding digital inclusion, it is necessary to work on a policy of implementation of **ethnic digital communication**, where Afro-descendant peoples can develop their ancestral knowledge through digital tools; bolstering training processes and the production of digital content mindful of the

inclusion and preservation of their culture, with the participation of young people and communities seeking to improve living conditions and generating individual and collective opportunities.

Digital transformation must abide in its implementation by rules that allow for **reliable and responsible AI**, with verifiable and auditable algorithms developed using databases without biases and prejudices. Otherwise, it will expand and reinforce inequality and marginalization.

Digital transformation must consider **decentralizing** data and information to avoid control and manipulation.

Digital transformation must promote the creation of **open-source** tools in order to make cost-free tools available to local, regional, and national governments and thereby enhance the effectiveness of their actions. It is also important to develop an **entrepreneurial ecosystem** by providing government support for seed projects for innovative, dynamic, and high-social-impact projects. Simultaneously, physical education, mathematics, and engineering should be strengthened, and an effort made to ensure cross-cutting innovation and technology in other areas.

Digital transformation must recognize the **right to identity**. All citizens must have access to their IDs and citizenship, and these must not be curtailed for political reasons. The diaspora must have the right to vote (e-democracy), using digital technologies and databases that protect identities.

Digital transformation must be developed together with policies to prevent cybercrime and generate a **digital security** context that ensures, inter alia, the right to privacy.

Digital transformation requires new regulatory frameworks and public policies for the **prevention of digital violence**, in order to safeguard human rights, with a clear gender focus, avoiding polarization and manifestations of authoritarianism, discrimination, hatred, harassment, extortion, aggression, incitement to violence, and defamation through technologies, all of which impair people's physical and mental integrity. Digital violence is also expressed by ignoring the role of various social actors, by the prevalence of misinformation, and in multiple ways that require interdisciplinary approaches. Likewise, in addition to prevention, it is also necessary to establish reporting mechanisms to ensure access to justice in the event of digital violence. A differential perspective is needed for all of the above, given the specific effects that hate speech has on women, ethnic minorities, and people of diverse sexual orientations.

Digital transformation must consider risks in **digital justice** mechanisms. Regulatory frameworks and processes must be generated to guarantee human rights in this context, including the right to privacy, transparency, access to information, and access to justice, the right to due process, to an adequate defense, and to legal assistance, particularly for vulnerable groups.

Digital transformation should favor **open government** practices at all levels of government, with readily available open data, accessibility, interoperability and reusability, to guarantee the right to public information and favor accountability and social and economic values, while ensuring the protection of privacy.

Digital transformation has an important role to play in **efforts to combat corruption**. Digital platforms for public integrity enhance the quality of our democracies.

Digital transformation must recognize the central role of **digital education**, with a gender focus and within a framework of interculturality, for social inclusion, universalization of the right to education, the right to academic freedom, and access to knowledge, including understanding new forms of learning in contexts of free access to information as well as broad access to the Internet, new technologies, digital libraries, and online publications; and guaranteeing copyright. At this point, it is essential to guarantee digital training for teachers who are not necessarily familiar with digital techniques, as well as the delivery of sufficient efficient and quality tools and/or equipment, including technical support for their maintenance.

Digital transformation should help to build an **intelligent citizenry**, focused on social innovation, with broad information distribution channels and networks and a global approach. Another proposal is to create **smart cities**, in which the efficient and intelligent use of technology becomes one of their most important pillars. Along the same lines, useful technological solutions need to be designed to ensure intelligent implementation of policies to overcome global challenges and ensure sustainable living. These solutions have two characteristics: they are smart (they solve everyday problems), and they are cheap (feasible, affordable, practicable, and replicable). The creation of smart cities is based on the following pillars: 1) Evidence-based public policies, 2) A focus on people and their quality of life, 3) Substantiated and sustainable decisions, 4) Technology (efficient and intelligent use), 5) Global vision. As a result, the city will improve its administrative management, increase its competitiveness and economic development, and reduce inequality gaps.

Digital transformation should take advantage of the new digital channels for local democratic participation as a way to improve the prioritization of **public investments**.

Digital transformation must place **technology at the service of people with disabilities**, in order to improve their quality of life by enabling access to health, rehabilitation, support, education, and employment, so that they can live their lives with equal rights and in dignity.

Digital transformation is dynamic and thus requires permanent follow-up of the commitments made at the Ninth Summit of the Americas, which is why civil society actors and organizations propose the creation of the **Digital Transformation Observatory of the Americas.** This observatory should include the participation of actors from the public sector, private business, civil society, and social actors, and publish annual progress reports and updates of its priorities in accordance with the interests of the different stakeholders. The observatory will be able to provide recommendations and follow up on the adoption of regional public policies with a focus on: i) the development of digital culture, ii) education and digital literacy, iii) greater participation of young people in cyber diplomacy, and iv) commitments to reduce gender gaps in digital education. In addition, joint regional cooperation can be advanced for the prevention of cyberbullying and all forms of digital violence, and for greater access to the Internet in rural areas.